UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/656,858	09/05/2003	Sonia Reed	016222-012810US	8576

20350	7590	03/06/2006

TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER
DWIVEDI, MAHESH H

ART UNIT	PAPER NUMBER
2168	

DATE MAILED: 03/06/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Application No.	Applicant(s)
Office Action Summary	10/656,858	REED ET AL.
	Examiner	Art Unit	
	Mahesh H. Dwivedi	2168	

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>05 September 2003</u>.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-57</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-57</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>02 February 2004</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date <u>12/6/2004</u>.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

Information Disclosure Statement

1.   The information disclosure statements (IDS) submitted on 12/06/2003 and

12/23/2003 have been received, entered into the record, and considered. The

submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the

information disclosure statement is being considered by the examiner.

Claim Rejections - 35 USC § 102

2.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public
>
> use or on sale in this country, more than one year prior to the date of application for patent in the United
>
> States.

3.   Claims 1-8, 12-17, 19-27, 31-36, 38-46, 50-55, and 57 are rejected under 35

U.S.C. 102(b) as being anticipated by **Carlisle et al.** ("Carlisle" (U.S. Patent

5,649,118)).

4.   Regarding claim 1, **Carlisle** teaches a system comprising:

A) a client having a plurality of applications residing thereon (Column 12, lines 60-63);

and

B) a secure token having a storage architecture (Column 4, lines 18-26), wherein the

storage architecture includes:

C) a directory and one or more attributes associated with the directory (Column 4, lines 18-26), wherein the one or more attributes associated with the directory are used to control access to the directory by the plurality of applications (Column 5, lines 20-30, Figure 2);

D) one or more cell groups under the directory (Column 4, lines 18-26), each cell group having one or more associated attributes, wherein the one or more attributes associated with a cell group are used to control access to that cell group by the plurality of applications (Column 5, lines 20-30, Figure 2); and

E) one or more cells under each cell group (Column 4, lines 18-26), each cell having one or more associated attributes, wherein the one or more attributes associated with a cell are used to control access to that cell by the plurality of applications (Column 5, lines 20-30, Figure 2).

The examiner notes that "password" (Column 5, line 23) is analogous to an **"attribute"**.

Regarding claims 2, 21, and 40, **Carlisle** further teaches a system, secure token, and method comprising:

A) wherein the one or more attributes associated with the directory permit access to the directory by one application and deny access to the directory to another application (Column 5, lines 20-30, Figure 2).

Regarding claims 3, 22, and 41, **Carlisle** further teaches a system, secure token, and method comprising:

A) wherein the one or more attributes associated with the cell group permit access to that cell group by one application and deny access to that cell group to another application (Column 5, lines 20-30, Figure 2).

Regarding claims 4, 23, and 42, **Carlisle** further teaches a system, secure token, and method comprising:

A) wherein the one or more attributes associated with the cell permit access to that cell by one application and deny access to that cell to another application (Column 5, lines 20-30, Figure 2).

Regarding claims 5, 24, and 43, **Carlisle** further teaches a system, secure token, and method comprising:

A) wherein one or more additional cell groups are added to the directory subsequent to issuance of the secure token to a token holder (Column 14, lines 60-67-Column 15, lines 1-10).

Regarding claims 6, 25, and 44, **Carlisle** further teaches a system, secure token, and method comprising:

A) wherein ownership of one of the one or more cell groups is determined subsequent

to issuance of the secure token to a token holder (Column 14, lines 60-67-Column 15,

lines 1-10).

Regarding claims 7, 26, and 45, **Carlisle** further teaches a system, secure token,

and method comprising:

A) wherein ownership of one of the one or more cell groups is modified subsequent to

issuance of the secure token to a token holder (Column 14, lines 60-67-Column 15,

lines 1-10).

Regarding claims 8, 27, and 46, **Carlisle** further teaches a system, secure token,

and method comprising:

A) wherein one or more additional cells are added to a cell group subsequent to

issuance of the secure token to a token holder (Column 14, lines 60-67-Column 15,

lines 1-10).

Regarding claims 12, 31, and 50, **Carlisle** further teaches a system, secure

token, and method comprising:

A) wherein the one or more attributes associated with a cell further control operations

on contents of that cell by the plurality of applications (Column 16, lines 65-67-Column

17, lines 1-19).

Regarding claims 13, 32, and 51, **Carlisle** further teaches a system, secure token, and method comprising:

A) wherein the one or more attributes associated with the cell permit a first set of operations on the contents of that cell by a first application (Column 16, lines 65-67-Column 17, lines 1-19);

B) wherein the one or more attributes associated with the cell permit a second set of operations on the contents of that cell by a second application (Column 16, lines 65-67-Column 17, lines 1-19); and

C) wherein the first set of operations is different from the second set of operations (Column 16, lines 65-67-Column 17, lines 1-19).

Regarding claims 14, 33, and 52, **Carlisle** further teaches a system, secure token, and method comprising:

A) wherein the one or more attributes associated with the directory permit a first application to access the directory after a first access condition is satisfied (Column 16, lines 65-67-Column 17, lines 1-19);

B) wherein the one or more attributes associated with the directory permit a second application to access the directory after a second access condition is satisfied (Column 16, lines 65-67-Column 17, lines 1-19); and

C) wherein the first access condition is different from the second access condition (Column 16, lines 65-67-Column 17, lines 1-19).

Regarding claims 15, 34, and 53, **Carlisle** further teaches a system, secure

token, and method comprising:

A) wherein the one or more attributes associated with the cell group permit a first

application to access that cell group after a first access condition is satisfied (Column

16, lines 65-67-Column 17, lines 1-19);

B) wherein the one or more attributes associated with the cell group permit a second

application to access that cell group after a second access condition is satisfied

(Column 16, lines 65-67-Column 17, lines 1-19); and

C) wherein the first access condition is different from the second access condition

(Column 16, lines 65-67-Column 17, lines 1-19).

Regarding claims 16, 35, and 54, **Carlisle** further teaches a system, secure

token, and method comprising:

A) wherein the one or more attributes associated with the cell permit a first application

to access that cell after a first access condition is satisfied (Column 16, lines 65-67-

Column 17, lines 1-19);

B) wherein the one or more attributes associated with the cell permit a second

application to access that cell after a second access condition is satisfied (Column 16,

lines 65-67-Column 17, lines 1-19); and

C) wherein the first access condition is different from the second access condition

(Column 16, lines 65-67-Column 17, lines 1-19).

Regarding claims 17, 36, and 55, **Carlisle** further teaches a system, secure

token, and method comprising:

A) wherein the secure token is a smart card (Column 4, lines 18-26).

Regarding claims 19, 38, and 57, **Carlisle** further teaches a system, secure

token, and method comprising:

A) wherein the smart card is a static or native smart card (Carlisle, Figure 2).

Regarding claims 20 and 39, **Carlisle** teaches a secure token and method

comprising:

A) a directory and one or more attributes associated with the directory (Column 4, lines

18-26), wherein the one or more attributes associated with the directory are used to

control access to the directory by the plurality of applications (Column 5, lines 20-30,

Figure 2);

B) one or more cell groups under the directory (Column 4, lines 18-26), each cell group

having one or more associated attributes, wherein the one or more attributes associated

with a cell group are used to control access to that cell group by the plurality of

applications (Column 5, lines 20-30, Figure 2); and

C) one or more cells under each cell group (Column 4, lines 18-26), each cell having

one or more associated attributes, wherein the one or more attributes associated with a

cell are used to control access to that cell by the plurality of applications (Column 5,

lines 20-30, Figure 2).

Claim Rejections - 35 USC § 103

5.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
>
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
>
> the prior art are such that the subject matter as a whole would have been obvious at the time the
>
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
>
> Patentability shall not be negatived by the manner in which the invention was made.

6.   This application currently names joint inventors. In considering patentability of

the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of

the various claims was commonly owned at the time any inventions covered therein

were made absent any evidence to the contrary. Applicant is advised of the obligation

under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was

not commonly owned at the time a later invention was made in order for the examiner to

consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g)

prior art under 35 U.S.C. 103(a).

7.   Claims 9-11, 28-30, and 47-49 are rejected under 35 U.S.C. 103(a) as being

unpatentable over **Carlisle et al.** (U.S. Patent 5,649,118) as applied to claims 1-8, 12-

17, 19-27, 31-36, 38-46, 50-55, and 57 above and in view of **Deo et al.** (U.S. Patent

6,970,891).

8.   Regarding claims 9, 28, and 47, **Carlisle** does not explicitly teach a system,

secure token, and method comprising:

A) wherein the one or more attributes associated with the directory are modified in

terms of permitting or denying access to the directory by the plurality of applications.

Deo, however, teaches **"wherein the one or more attributes associated with**

the directory are modified in terms of permitting or denying access to the

directory by the plurality of applications" as "the file system includes an ACL

(access control list) that performs the security function of determining which users

and/or applications have access to which files" (Column 4, lines 37-44).

It would have been obvious to one of ordinary skill in the art at the time the

invention was made to combine the teachings of the cited references because teaching

Deo's would have allowed **Carlisle's** to provide a method to render data in volatile

memory available to multiple applications in a simple way, but in a secure fashion to

protect against unintentional usage by rogue or malicious applications, as noted by **Deo**

(Column 1, lines 29-32).

Regarding claims 10, 29, and 48, **Carlisle** does not explicitly teach a system,

secure token, and method comprising:

A) wherein the one or more attributes associated with a cell group are modified in terms

of permitting or denying access to that cell group by the plurality of applications.

Deo, however, teaches **"wherein the one or more attributes associated with a cell group are modified in terms of permitting or denying access to that cell group by the plurality of applications"** as "the file system includes an ACL (access control list) that performs the security function of determining which users and/or applications have access to which files" (Column 4, lines 37-44).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Deo's** would have allowed **Carlisle's** to provide a method to render data in volatile memory available to multiple applications in a simple way, but in a secure fashion to protect against unintentional usage by rogue or malicious applications, as noted by **Deo** (Column 1, lines 29-32).

Regarding claims 11, 30 and 49 **Carlisle** does not explicitly teach a system, secure token, and method comprising:

A) wherein the one or more attributes associated with a cell are modified in terms of permitting or denying access to that cell by the plurality of applications.

Deo, however, teaches **"wherein the one or more attributes associated with a cell are modified in terms of permitting or denying access to that cell by the plurality of applications"** as "the file system includes an ACL (access control list) that performs the security function of determining which users and/or applications have access to which files" (Column 4, lines 37-44).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Deo's** would have allowed **Carlisle's** to provide a method to render data in volatile memory available to multiple applications in a simple way, but in a secure fashion to protect against unintentional usage by rogue or malicious applications, as noted by **Deo** (Column 1, lines 29-32).

9.   Claims 18, 37, and 56 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Carlisle et al.** (U.S. Patent 5,649,118) as applied to claims 1-8, 12-17, 19-27, 31-36, 38-46, 50-55, and 57 above and in view of **Wentker et al.** (U.S. Patent 6,481,632).

Regarding claims 18, 37 and 56, **Carlisle** does not explicitly teach a system, secure token, and method comprising:

 A) wherein the smart card is an open platform smart card.

   Wentker, however, teaches **"wherein the smart card is an open platform smart card"** as "open platform architecture" (Column 5, lines 59-67).

   It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Wentker's** would have allowed **Carlisle's** to provide a method to manage and change the content of cards wile allowing for the flexibility to share control of the card with other business entities, as noted by **Wentker** (Column 5, lines 66-67-Column 6, lines 1-2).

Conclusion

10.   The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Patent 6,199,762 issued to **Hohle** on 13 March 2001. The subject matter disclosed therein is pertinent to that of claims 1-59 (e.g., methods to secure and use smart cards).

U.S. Patent 6,367,011 issued to **Lee et al.** on 02 April 2002. The subject matter disclosed therein is pertinent to that of claims 1-59 (e.g., methods to secure and use smart cards).

U.S. Patent 5,682,027 issued to **Bertina et al.** on 28 October 1997. The subject matter disclosed therein is pertinent to that of claims 1-59 (e.g., methods to secure and use smart cards).

Contact Information

11.   Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mahesh Dwivedi whose telephone number is (571) 272-2731. The examiner can normally be reached on Monday to Friday 8:20 am – 4:40 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tim Vo can be reached (571) 272-3642. The fax number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the
Patent Application Information Retrieval (PAIR) system. Status information for
published applications may be obtained from either Private PAIR or Public PAIR.
Status information for unpublished applications is available through Private PAIR only.
For more information about the PAIR system, see http://pair-direct.uspto.gov. Should
you have questions on access to the Private PAIR system, contact the Electronic
Business Center (EBC) at 866-217-9197 (toll-free).

Mahesh Dwivedi

Patent Examiner

Art Unit 2168

February 27, 2006
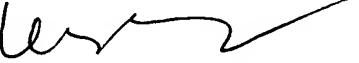
Leslie Wong

Primary Examiner